UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/827,167	04/19/2004	James M. Alkove	MSFT-3491	2413

41505 7590 07/02/2007

WOODCOCK WASHBURN LLP (MICROSOFT CORPORATION)
CIRA CENTRE, 12TH FLOOR
2929 ARCH STREET
PHILADELPHIA, PA 19104-2891

EXAMINER	
ZEE, EDWARD	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
07/02/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/827,167	ALKOVE ET AL.	
	Examiner	Art Unit	
	Edward Zee	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 April 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *19 April 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *8/30/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the original filing on April 19th, 2004. Claims 1-20 are pending and have been considered below.

Claim Objections

2. Claims 8-11 and 13 are objected to because of the following informalities: the examiner notes the use of acronyms (ie. MAC, ID) throughout these claims without first including a description in plain text, as required. Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claim 11 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

5. Claim 11 recites the limitation "the first and second nonces" in line 20. There is insufficient antecedent basis for this limitation in the claim. The examiner will interpret this as "a first and second nonce" when examining the claim below.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 7 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thoma et al. (2002/0152393).

Claim 1: Thoma et al. discloses a method in connection with a first computing device (`transmitter`) and a second computing device (`receiver`) interconnected by a network, the transmitter for transmitting protected digital content to the receiver in a manner so that the receiver can access the content, the content being encrypted and decryptable according to a content key (KD), the method comprising:

a. the receiver*(terminal device)* sending an session request*(transfer ticket)* to the transmitter*(content server)*, the session request including an identification of the content*(e-content's license ID)* to the transmitter, an action to be taken with the content*(register license so that content can be consumed at the terminal device)*, and a unique identification of the receiver*(dedicated device ID)* [pages 5-6, paragraphs 0061-0062];

b. the transmitter*(content server)* receiving the session request from the receiver*(terminal device)*, determining from the unique identification of the receiver in the session request that the receiver is in fact registered to the transmitter*(checks if there is an entry for the e-content license/dedicated device ID pair in the license repository)*, obtaining a digital license corresponding to the identified content*(checks if the license has an owner assigned)* in the

session request, reviewing policy set forth in the license to determine that the license allows the transmitter to provide access to the content to the receiver and also allows the action in the session request*(checks if the transfer ticket counter matches)* [page 6, paragraph 0063];

c. and sending a session response to the receiver*(terminal device)*, the session response including the policy from the license*(serial counter)* and the unique identification of the receiver*(device ID)* [page 6, paragraph 0064];

d. the transmitter*(content server)* obtaining the content encrypted according to (KD)*(symmetric key)* to result in (KD(content))*(encrypts the content with symmetric key)*, and sending (KD(content) to the receiver along with the content key (KD) for decrypting the encrypted content, (KD) being protected in a form obtainable by the receiver*(license key encrypted with the public key)* [page 5, paragraph 0058-0059];

e. the receiver receiving the session response*(ie. upon receiving the transfer ticket and solved challenge)*, (KD(content))*(content encrypted with license key)* and the protected content key (KD)*(license key encrypted with public key)* for decrypting the encrypted content [page 5, paragraph 0059 & page 6, paragraph 0066];

f. and retrieving the policy from the session response, confirming that the policy allows the receiver to render the content*(terminal device checks if the challenge has been solved)*, obtaining the content key (KD), applying (KD) to (KD(content)) to reveal the content*(the private key is used to decrypt the license key, which in turn is used to decrypt the content)*, and then in fact rendering the content in accordance with the policy*(if equal, the active flag is set to activate the license)* [page 5, paragraph 0033 & page 6, paragraph 0066].

However, Thoma et al. does not explicitly disclose that the content key (KD) for decrypting the encrypted content is included in the session response provided by the transmitter to the receiver, instead it is sent with the encrypted content. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to include the content key in the initial session response or with any other response transmission. One would have been motivated to do so in order to simplify registration and license activation by transmitting all the required decryption keys and any other data required for consuming the protect content in a single data transmission.

Claim 7: Thoma et al. discloses a method as in claim 1 above and further discloses the transmitter encrypting the content key (KD) according to a public key of the receiver (PU-R) to result in (PU-R(KD))*(license key encrypted with the public key)*, the receiver decrypting the content key by applying a private key (PR-R) corresponding to (PU-R) to (PU-R(KD)) to result in (KD) [page 5, paragraph 0059], but does not explicitly disclose the transmitter having it's own public/private key pair (PU-X, PR-X) which is applied when retrieving the content key (KD) in an encrypted format (PU-X(KD)) by decrypting the content key with it's private key (PR-X). However, it would have been obvious to one of ordinary skill in the art at the time of invention to store the content key in an encrypted fashion and to decrypt this key at the time of use. One would have been motivated to do so in order to further enhance the security of the system by encrypting all sensitive data before storing it, which will prevent potential hackers from obtaining sensitive data, such as a content key, even if they successfully infiltrate the data store containing the content key.

Claim 8: Thoma et al. discloses a method as in claim 1 above and further discloses the transmitter*(content server)* digitally signing policy information*(free form data structure is signed*

with the terminal device's private key) and sending this to the receiver*(terminal device)* [page 5, paragraph 0060], but does not explicitly disclose digitally signing the session response, which binds the policy to the session response, and further including the signature with the response. However, it would have been obvious to one of ordinary skill in the art at the time of invention to digitally sign the session response, and including the signature with the response. One would have been motivated to do so in order to prevent the end user from modifying or faking any policy information.

8. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Thoma et al. (2002/0152393) in view of Weber (2004/0098583).

Claim 2: Thoma et al. discloses a method as in claim 1 above and further discloses:

a. the transmitter*(content server)* in conjunction with sending the session response also storing at least a portion of the session request*(license repository stores information for each copy of e-content downloaded including terminal device ID)* and at least a portion of the session response*(ie. license key)* in a transmitter session store*(license repository)* [page 5, paragraphs 0055 & 0058]. The examiner notes that the terminal device ID is part of the initial session request;

b. the receiver*(terminal device)* receiving the session response from the transmitter and storing in a receiver session store*(license table)* information about the licenses that are registered for the receiver [page 3, paragraph 0036];

c. and the receiver sending a transfer request to the transmitter*(to download encrypted content the terminal device sends a request to the content server)*; and the transmitter receiving the transfer request, retrieving from the transfer request the identification of the content*(the*

request is received by the content server and includes a unique ID for content requested), obtaining the content encrypted according to (KD) to result in (KD(content)), and sending a transfer response to the receiver including (KD(content))*(the content server sends a response to the terminal device, which includes the content encrypted with the license key)* [page 5, paragraphs 0058-0059].

However, Thoma et al. does not explicitly disclose:

a. the receiver first receiving the initial session response from the transmitter and storing at least a portion of the session response in a receiver session store and the receiver retrieving at least a portion of the session response from the receiver session store, before sending a transfer request to the transmitter based on the session response;

b. and the transmitter receiving the transfer request and retrieving the at least a portion of the session request and at least a portion of the session response from the transmitter store based on the transfer request, retrieving from the retrieved at least a portion of the session request and at least a portion of the session response the identification of the content, before obtaining the encrypted content and sending a transfer response to the receiver including (KD(content)).

Nonetheless, Weber discloses a similar method and further discloses performing an initial session request*(upon receipt of the request for digital content, the sending device replies to the receiving device with a request for an acknowledgment)* to verify the user before sending protected content to the user [page 2, paragraph 0015].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to first complete an initial session request(ie. license registration, proximity test, etc.) before initiating a request for protected content and performing a transmission of the protected

content to the end user disclosed by Thoma et al.. One would have been motivated to do so in order to further prevent unauthorized use of protected digital content by first verifying that a particular user is allowed to download such content(ie. license registration) before transmitting the content to the user. The examiner notes that even though the content is cryptographically protected, there is still a possibility that an unauthorized end user may defeat such encryption techniques and utilize the digital content.

9. Claims 3 and 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thoma et al. (2002/0152393) in view of Messerges et al. (2002/0157002).

Claims 3 and 4: Thoma et al. discloses a method as in claim 1 above and further discloses that the receiver*(terminal device)* sending the session request*(transfer ticket)* further includes a unique serial number, which is used by the transmitter*(content server)* to check if the session request is initiated from an authorized receiver*(content server checks if the transfer ticket counter matches the value in the license repository, if not the transfer ticket has already been used to activate this license)* [page 6, paragraphs 0062-0063]. However, Thoma et al. does not explicitly discloses that the receiver sending the session request further including a version number of a revocation list of the receiver (V-RL-R), and the transmitter sending the session response further including a version number of a revocation list of the transmitter (V-RL-X), the method further comprising the receiver determining that (V-RL-R) is more current than (V-RL-X) and sending the revocation list thereof to the transmitter. Furthermore, Thoma et al. does not explicitly disclose that the receiver sending the session request further including a version number of a revocation list of the receiver (V-RL-R), and the transmitter determining that a version number of a revocation list thereof (V-RL-X) is more current than (V-RL-R) and sending

the revocation list thereof to the receiver. Nonetheless, Messerges et al. discloses a similar method and further discloses the use of a revocation list*(domain authority checks revocation list)* to determine if a user requesting content is currently a valid user, and a revocation detector to update the revocation list*(domain authority keeps a list of revoked users)* [page 3, paragraph 0029 and page 8, paragraph 0071]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to employ a revocation list when the transmitter, disclosed by Thoma et al., is verifying the validity of the receiver and to further maintain and utilize the most recent revocation list version. One would have been motivated to do so in order to further prevent unauthorized use of protected digital content.

10. Claims 5, 6, 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thoma et al. (2002/0152393) in view of Arthan (6,754,349).

Claims 5 and 6: Thoma et al. discloses a method as in claim 1 above and further discloses the transmitter*(content server)* maintain a database*(key server)* of receivers*(terminal devices)* public/private key pair and sending a session response to the receiver including the content key (KD)*(license key)* for decrypting the content encrypted according to (PU-R)*(license key encrypted with the public key)* [page 5, paragraph 0058-0059], but does not explicitly disclose the receiver sending a session request to the transmitter including a public key of the receiver (PU-R); nor the transmitter alternatively sending a seed, from which the content key may be derived, in place sending the actual content key itself. However, Arthan discloses a similar method and further discloses using a seed value to generate an encryption key and encrypting data with this key and later using this seed value to generate the decryption key and using the key to decrypt the encrypted data [column 1, lines 15-31].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include the public key in the session request. One would have been motivated to do so in order to minimize the amount of storage space required by the digital rights management system by sending the user's public key to the transmitter instead of storing these keys in a database, which in turn would require substantially more memory.

Furthermore, it is old and well known in the cryptographic art to employ a seed for generating an encryption key and later using the seed to generate the decryption key and would have been obvious to one of ordinary skill in the art at the time of invention to utilize a seed, from which the content key may be derived, and transmit this in place of the actual content key. One would have been motivated to do so in order to increase the security of the system by making it more difficult for an eavesdropper to identify the encryption key.

Claims 9 and 10: Thoma et al. discloses a method as in claim 8 above and further discloses the transmitter sending a session response to the receiver including a signature/MAC based on a private key of the receiver (PR-R)*(content server signs free form data with receiver's private key)*, the receiver receiving the session response from the transmitter and verifying the signature/MAC of the session response using the public key of the receiver (PU-R)*(free form data to be read with the public key)* [page 5, paragraph 0060]. However, Thoma et al. does not explicitly disclose basing the signature/MAC on a symmetric integrity key (KI), the session response further including (KI) encrypted according to a public key of the receiver (PU-R) to result in (PU-R(KI)), the method also comprising the receiver receiving the session response from the transmitter, retrieving (PU-R(KI)) therefrom, applying a private key (PR-R) corresponding to (PU-R) to (PU-R(KI)) to result in the (KI), and verifying the signature/MAC of

the session response based on (KI); nor alternatively employing a seed, from which a symmetric integrity key can be derived, and transmitting the seed instead of the integrity key itself.

However, it would have been obvious to one of ordinary skill in the art at the time of invention to base a digital signature/MAC on a symmetric key or any other encryption key and to further encrypt the key of which the signature/MAC is based on. One would have been motivated to do so in order to increase the integrity of the system by adding and additional layer of encryption to the verification process.

Furthermore, Arthan discloses a similar method and further discloses using a seed value to generate an encryption key and encrypting data with this key and later using this seed value to generate the decryption key and using the key to decrypt the encrypted data [column 1, lines 15-31]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to utilize a seed, from which the content key may be derived, and transmit this in place of the actual content key. One would have been motivated to do so in order to increase the security of the system by making it more difficult for an eavesdropper to identify the encryption key.

11. Claims 11-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Thoma et al. (2002/0152393), Messerges et al. (2002/0157002) and Weber (2004/0098583) as applied to claim 11 above, and further in view of Montero (6,133,912).

Claim 11: Thoma et al. discloses a method as in claim 1 above and further discloses the receiver registering with the transmitter by:

a. the receiver*(terminal device)* sending a registration request*(initial registration of new license: ie. transfer ticket)* to the transmitter, the registration request including the unique identification of the receiver*(dedicated device ID)* [page 6, paragraph 0062];

b. the transmitter validating the registration request*(content server performs a series of checks: ie. if entry exists in license repository, if license is assigned already, if counter matches, etc.)* [page 6, paragraph 0063];

c. the transmitter*(content server)* sending a registration response to the receiver, the registration response including the unique identification of the receiver and a decrypted random number(ie. nonce) [page 6, paragraph 0064], but does not explicitly disclose the transmitter's registration response includes a registration ID generated by the transmitter to identify the registration response.

However, Messerges et al. discloses a similar method and further discloses a registration response to the receiver*(user device)*, which includes a registration ID*(provides them with a domain ID)* generated by the transmitter*(domain authority)* [page 4, paragraphs 0035-0036]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to include a registration ID with the registration response disclosed by Thoma et al.. One would have been motivated to do so in order to assure content providers that no fraudulent users are registered and allowed access to protected content. For example, this may be accomplished by generating registration IDs, which comprise of serial numbers and cryptographic elements, thus making it extremely difficult to counterfeit, and further binding these registration IDs to the distributed protected content.

Nonetheless, neither Thoma et al. nor Messerges et al. explicitly disclose utilizing a proximity requirement to further prevent unauthorized access by performing the steps of:

a. the receiver sending a port address of a port thereof and the registration ID to the transmitter;

b. the transmitter sending a proximity message to the receiver by way of the sent port address and concurrently noting a start time;

c. the receiver upon receiving the proximity message at the port address thereof employing at least a portion of the registration response and the proximity message to generate a proximity value and sending a proximity response with the proximity value to the transmitter;

d. and the transmitter receiving the proximity response with the proximity value from the receiver and concurrently noting an end time, verifying the proximity value based on a first and second nonce, calculating from the noted start and end times an elapsed time, comparing the elapsed time to a predetermined threshold value, deciding from the comparison that the receiver satisfies a proximity requirement, and registering the receiver as being able to access content from such transmitter.

However, Weber discloses a similar method and further discloses utilizing a proximity requirement to prevent unauthorized users from accessing protected digital content by performing the steps of:

a. the receiver*(receiving device)* sending a port address*(the physical address is known to the sending device)* and a secret(ie. secret keys or unique identifying information such as a registration ID) to the transmitter*(receiving device uses secrets or secret keys to convince the sending device that they are authorized)* [page 2, paragraphs 0016 & 0020]. The examiner notes

that the transmitter knowing the port address of the receiver implies that this address has to have been sent to the transmitter at some point in time;

b. the transmitter*(sending device)* sending a proximity message to the receiver by way of the sent port address*(sending device sends a request for an acknowledgement from receiving device)* and concurrently noting a start time*(the request for acknowledgment is sent at time T1)* [page 2, paragraphs 0015 & 0020];

c. the receiver*(receiving device)* upon receiving the proximity message at the port address thereof employing the proximity message to generate a proximity value and sending a proximity response with the proximity value to the transmitter*(receiving device sends the requested acknowledgment to the sending device)* and the transmitter receiving the proximity response with the proximity value from the receiver and concurrently noting an end time*(the acknowledgment is received by the sending device at T2)*, calculating from the noted start and end times an elapsed time*(sending device calculates an actual round-trip response time)*, comparing the elapsed time to a predetermined threshold value*(compares the actual response time to the predetermined response time limit)*, deciding from the comparison that the receiver satisfies a proximity requirement*(comparing the actual response time to the predetermined response time limit, the sending device is able to determine if receiving device is located within the predetermined distance)*, and registering the receiver as being able to access content from such transmitter*(if the receiving device is within the predetermined distance from sending device, sending device grants the requests)* [page 2, paragraphs 0015-0016 & 0020], but does not explicitly disclose the transmitter sending cryptographic elements(ie. first and second nonce) to the receiver in order to facilitate digitally signing the proximity response before sending it back

to the transmitter, and furthermore the transmitter verifying the response before allowing registration to the receiver.

Furthermore, Montero discloses a similar method and further discloses the act of encrypting and or digitally signing a ping signal [column 12, lines 18-24].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to utilize a proximity requirement while determining the authenticity of the registration request disclosed by Thoma et al. and Messerges et al. and additionally perform the required steps to encrypt and or digitally sign the response values transmitted during the proximity test. One would have been motivated to do so in order to increase security by incorporating additional levels of authentication and protection. For example, preventing unauthorized devices from using a compromised secret key to obtain protected digital content by determining that the device is situated at a physical location further than the predetermined distance for the particular secret key in use.

Claim 12: Thoma et al., Messerges et al., Weber and Montero disclose a method as in claim 11 above and Thoma et al. further discloses the receiver sending a registration request, which is digitally signed with its private key, to the transmitter and the transmitter verifying this request by decrypting the request with the receiver's public key [page 6, paragraph 0062-0063], but does not explicitly disclose:

a. the receiver sending a registration request to the transmitter including a digital certificate provided to the receiver by an appropriate certifying authority, the certificate including therein a public key of the receiver (PU-R) and a digital signature;

b. the method also comprising the transmitter validating the certificate and verifying with reference to a revocation list that the certificate has not been revoked.

However, Messerges et al. discloses a similar method and further discloses the receiver*(user device)* sending a registration request to the transmitter including a digital certificate provided to the receiver by an appropriate certifying authority, the certificate including therein a public key of the receiver (PU-R) and a digital signature*(when a user wishes to enroll a user device into a domain, the user device and the domain authority engage in a protocol to authenticate each other)*, the method also comprising the transmitter validating the certificate and verifying with reference to a revocation list*(the domain authority may also check a revocation list)* that the certificate has not been revoked [page 4, paragraph 0041 & page 3, paragraph 0029].

Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to additionally employ a certificate authority and revocation list while determining the authenticity of the registration request disclosed by Thoma et al.. One would have been motivated to do so in order to increase security by incorporating additional levels of authentication and protection.

Claim 13: Thoma et al., Messerges et al., Weber and Montero disclose a method as in claim 11 above and Thoma et al. further discloses the receiver sending a registration request to the transmitter including a device ID*(unique device ID)* of the receiver [page 6, paragraph 0062].

Claim 14: Thoma et al., Messerges et al., Weber and Montero disclose a method as in claim 11 above and Thoma et al. further discloses the receiver sending a registration request, which includes a portion that is encrypted with the private key (PR-R)*(transfer ticket)* and a portion that

is encrypted with its public key*(challenge)*, to the transmitter and the transmitter decrypting the registration request portion by application of corresponding public and private keys [page 6, paragraph 0062-0063], but does not explicitly disclose the receiver sending a registration request to the transmitter including a public key of the receiver (PU-R), and comprising the transmitter encrypting at least a portion of the registration response by (PU-R) and the receiver decrypting the registration response by application of a private key (PR-R) corresponding to (PU-R).

However, it would have been obvious to one of ordinary skill in the art at the time of invention to encrypt the response to the receiver with the public key, private key or any other encryption key known to the transmitter. One would have been motivated to do so in order to increase the security of the system by minimizing the amount unencrypted data sent across an insecure connection.

Claims 15-18: Thoma et al., Messerges et al., Weber and Montero disclose a method as in claim 11 above, but Thoma et al. does not explicitly disclose:

a. the transmitter sending the registration response including a first nonce to the receiver;

b. the transmitter sending the proximity message with a second nonce to the receiver by way of the sent port address and concurrently noting the start time;

c. the receiver upon receiving the proximity message at the port address thereof employing the sent first and second nonces to generate the proximity value and sending the proximity response with the proximity value and the registration ID to the transmitter, wherein the receiver generates a proximity valve:

i. by employing the first nonce as a cryptographic key to perform an encryption of the second nonce and thus result in an encrypted value;

ii. by employing the first nonce as a cryptographic key to perform a hash over the second nonce and thus result in a hash value;

iii. by performing a hash over the first and second nonces to result in a hash value.

However, Montero discloses a similar method and further discloses encrypting and compressing the proximity messages and proximity values*(ping signal)* using standard encryption(ie. encryption with a key or keyed hash) and compression techniques(ie. hashing) [column 12, lines 18-24]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use nonces*(random values)* as cryptographic elements and provide these elements to the receiver to generate the proximity value in an encrypted fashion before sending the proximity value back to the transmitter for the purpose of concluding the proximity test disclosed by Thoma et al., Messerges et al. and Weber. One would have been motivated to do so in order to increase the integrity of the system by producing digitally verifiable response values and by further employing random numbers as encryption/decryption keys.

Claim 19: Thoma et al., Messerges et al., Weber and Montero disclose a method as in claim 11 above and Thoma et al. further discloses the transmitter registering the receiver by placing the unique identification of the receiver in a registry list*(license repository)*, and determining from the unique identification of the receiver in the session request with reference to the registry list that the receiver is in fact registered to the transmitter [page 5, paragraph 0055].

Claim 20: Thoma et al., Messerges et al., Weber and Montero disclose a method as in claim 11 above, but Thoma et al. does not explicitly disclose the transmitter periodically requiring the receiver to re-register by re-sending a registration request to the transmitter. However, it would have been obvious to one of ordinary skill in the art at the time of invention to periodically

require the receiver to re-register. One would have been motivated to do so in order to maintain integrity of the system.

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Lao (2002/0198846).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 9:00AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
June 20, 2007

Thanhnga B. Dang
AU2135